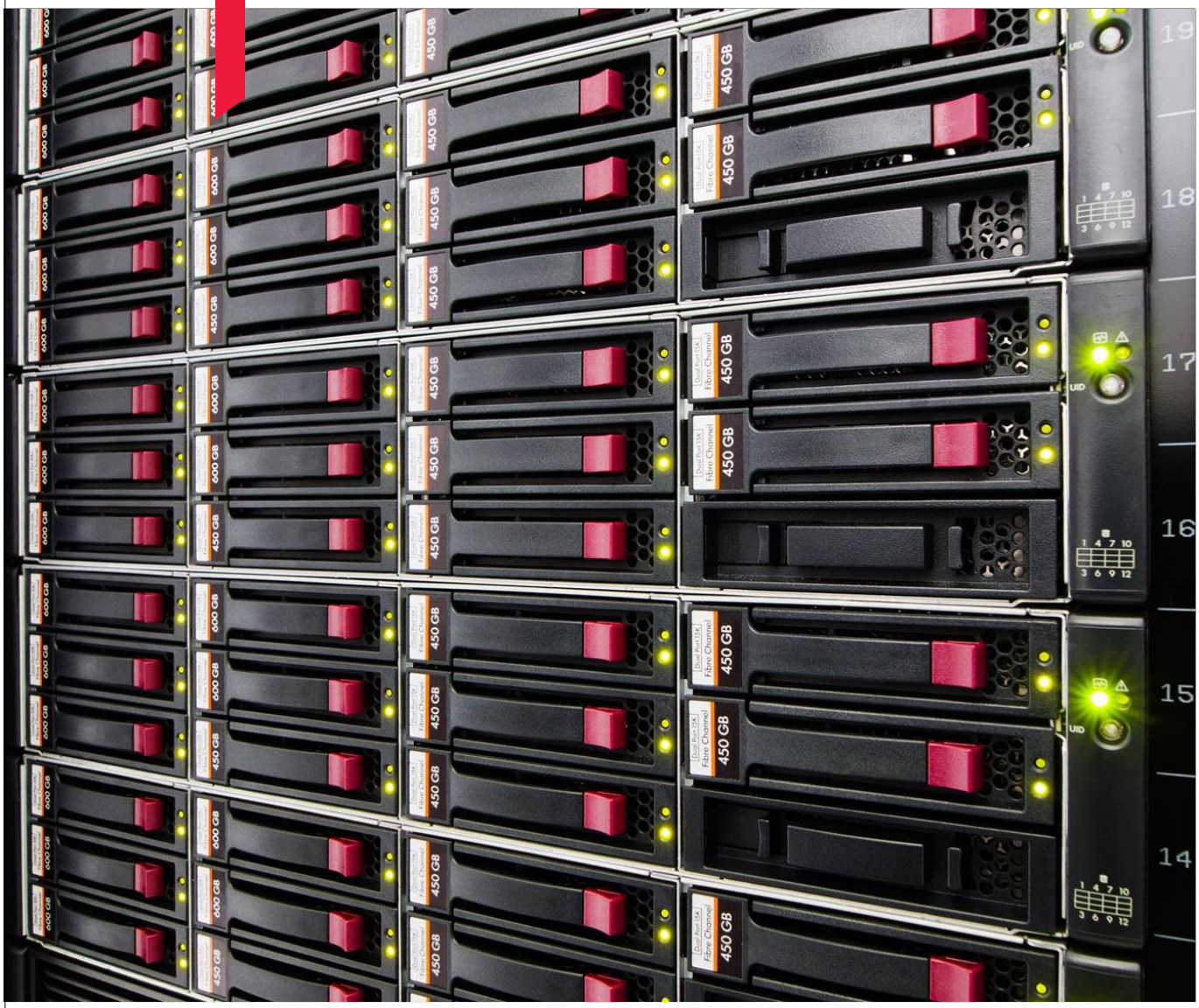

COMBY A/S

INDEPENDENT AUDITOR'S ISAE 3402 REPORT AT 30 NOVEMBER 2022 ON THE DESCRIPTION OF HOSTED AND MANAGED SERVICES AND THE RELATING CONTROLS AND THEIR DESIGN

CONTENTS

1. AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S ASSURANCE REPORT AT 30 NOVEMBER 2022 OF HOSTED AND MANAGED SERVICES AND THE RELATING CONTROLS AND THEIR DESIGN

To: The Management in COMBY A/S
COMBY A/S' customers and their auditors

Scope

We have been engaged to report on COMBY A/S' (the service provider) description in section 3 of hosted and managed services and related controls, and on the design and implementation of controls related to the control objectives stated in the description on 30 November 2022.

We have not performed procedures regarding the operating effectiveness of the controls stated in the description, and accordingly, we do not express an opinion on this.

The Service Provider's Responsibilities

The service provider is responsible for preparing the description and accompanying statement in section 2, including the completeness, accuracy, and method of presentation of the description and the statement.

The service provider is responsible for providing the services covered by the description; stating the control objectives; and identifying the risks threatening achievement of the control objectives; designing and implementing effectively operating controls to achieve the stated control objectives.

The information in section 5 - Supplementary information from COMBY A/S is not part of COMBY A/S' description of services. The information in section 5 has not been the subject of the procedures carried out by BDO when reviewing the description in section 3.

Auditor's Independence and Quality Assurance

We have complied with the requirements of independence and other ethical requirements of the International Ethics Standards Board of Auditors' International Guidelines on the Conduct of Auditors (IESBA Code), which are based on the fundamental principles of integrity, objectivity, professional competence, and due diligence, confidentiality, and professional conduct, as well as ethical requirements applicable in Denmark.

We are subject to the international standard on quality control, ISQC 1, and accordingly use and maintain a comprehensive system of quality control, including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Auditor's Responsibilities

Our responsibility is, on the basis of our actions, to express a conclusion about the service provider's description as well as about the design and operation of controls related to the control objectives set out in this description.

We have performed our work in accordance with International Standard on Assurance Engagements 3402 on declaration duties with security checks at a service organisation. This standard requires that we plan and carry out our actions in order to obtain a high degree of certainty as to whether the description is correct in all material respects and whether the controls in all essential respects are appropriately designed.

A declaration task with certainty to provide a statement about the description and design of controls at a service provider includes performing actions to obtain evidence of the information in the service provider's description as well as of the controls' design. The actions chosen depends on the assessment of the service provider's auditor, including the assessment of the risks that the description is not accurate and that the controls are not appropriately designed. An assurance engagement of this type further includes an assessment of the overall presentation of the description, the appropriateness of the control objectives set out therein and the appropriateness of the criteria specified and described by the service provider in section 2.

As described above, we have not performed procedures regarding the operating effectiveness of the controls stated in the description and, accordingly, we do not express an opinion on this.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Limitations of Controls at a Service Organisation

The service organisations' description is prepared to meet the common needs of a wide range of customers and their auditors and may not, therefore, include every aspect of hosted and managed services that each individual customer may consider important in its own particular environment. Also, because of their nature, controls at a service organisation may not prevent or detect all errors or omissions. Also, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at a service organisation may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion are those described in service providers statement in section 2. In our opinion, in all material respects:

a. The description presents fairly the controls relating to hosted and managed services as designed and implemented on 30 November 2022; and
b. The controls stated in the description were suitably designed and implemented on 30 November 2022.

Description of Tests of Controls

The specific controls tested, and results of those tests are listed in section 4.

Intended Users and Purpose

This report is intended only for customers, which have used the service provider's hosted and managed services, and their auditors who have a sufficient understanding to consider it, along with other information about controls operated by the customer themselves when obtaining an understanding of customers' information systems relevant to financial reporting.

Copenhagen, 16 January 2023

BDO Statsautoriseret revisionsaktieselskab

Nicolai T. Visti
Partner, State Authorised Public Accountant

Mikkel Jon Larssen
Partner, Head of Risk Assurance, CISA, CRISC

2. COMBY A/S' STATEMENT

COMBY A/S performs support and safeguard provision of IT operations to its customers.

The description has been prepared for COMBY A/S' customers and their auditors who have a sufficient understanding to consider hosted and managed services, along with other information, including information about controls operated by the customers themselves, when assessing the risks of material misstatements of customers' financial statements.

COMBY A/S confirms that the accompanying description in section 3 fairly presents controls in relation to hosted and managed services and associated controls on 30 November 2022. The criteria used in making this statement were that the accompanying description:

1. Explains regarding hosted and managed services, and how related controls were designed and implemented, including explaining:
    - The services provided, regarding the handled groups of transactions, when relevant.
    - The processes in both IT and manual systems that are used to initiate the records and process.
    - How the system handles other significant events and conditions than transactions.
    - Relevant control objectives and controls designed to achieve those objectives.
    - Controls that we have assumed would be implemented by the user companies with reference to the design of the system and which, if necessary to achieve the control objectives stated in the description, are identified in the description along with the specific control objectives we cannot reach ourselves.
    - Other aspects of our control environment, risk assessment process, information system (including the associated business processes) and communication, control activities and monitoring controls that have been relevant to the processing and reporting of customer transactions.

2. Does not omit or distort information relevant to the scope of the controls described relating to general hosted and managed services considering that the description is prepared to meet the general needs of a wide range of customers and their auditors and therefore cannot include every aspect of hosted and managed services that the individual customer may consider of importance to their special environment.

COMBY A/S confirms that controls related to the control objectives stated in the accompanying description were suitably designed at 30 November 2022. The criteria we used in making this statement were that:

1. The risks that threatened achievement of the control objectives stated in the description were identified.

2. The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved.

Slagelse, 16 January 2023

COMBY A/S

Stefan Boel
Chief Operating Officer, COMBY A/S

3. COMBY A/S' DESCRIPTION OF HOSTED AND MANAGED SERVICES

GENERAL DESCRIPTION OF COMBY A/S

This description is prepared for the purpose of reporting on the IT general controls that COMBY A/S applies to support and safeguard provision of IT operations to its customers. The description focuses on business-related control objectives and processes implemented to safeguard COMBY A/S' provision of IT operations.

DESCRIPTION OF COMBY A/S' IT SERVICES

COMBY A/S has since its foundation been an IT service provider. COMBY A/S' services is therefore either directly part of our managed services or as a supplement to our managed services. COMBY A/S has offices in both Greenland and Denmark and every service is delivered from both Greenland and Denmark through the same processes and guidelines. COMBY A/S delivers the following services to its customer:

- Operations and maintenance of desktops
- Operations and maintenance of servers
- Operations and maintenance of network equipment
- Server hosting
- ISP connections
- Service Desk
- Security services

Furthermore, COMBY A/S has business consultants to manage both simple and large IT implementation projects. As a part of this COMBY A/S has the knowledge to deliver the following business consultant services:

- Project Management (both traditional and agile)
- Product requirements and User requirements
- Business cases and Benefit realization

RISK MANAGEMENT OF COMBY A/S

Risk management is carried out on different parts of the organisation and at different levels on targeted systems and input for the assessments is obtained from all levels of the organisation.

The likelihood and consequence of the threats are reassessed based on the information existing at the present time. This reflects, in combination, the threat level. When the threat level is low, the need for security measures is lower than when the threat level is high. When the threat level has been determined, it is assessed to which extent the security environment considers the relevant threat level and if any actions are needed to tighten the security environment in order to adhere to the threat level.

On the operational level risk management activities is carried by the system owner for each system and is re-assessed yearly for each system.

This report includes solely controls and control objectives for processes and controls that are managed by COMBY A/S and, thus, it does not include controls or control objectives that are managed by sub-organisations.

CONTROL FRAMEWORK, CONTROL STRUCTURE AND CRITERIA FOR CONTROL IMPLEMENTATION

COMBY A/S' information security is defined on the basis of the objective to provide dedicated IT outsourcing and high-quality infrastructure solutions, including stability and security.

The determination of criteria and scope of control implementation at COMBY A/S is based on the ISO 27002:2013 framework for management of information security. The following control areas in ISO 27002 were assessed:

- A.5. Information security policy
- A.6. Organisation of information security
- A.7. Human resource security
- A.8. Asset management
- A.9. Access management
- A.11. Physical and environmental security
- A.12. Operations security
- A.13. Communications security
- A.16. Information security incident management
- A.17. Information security aspects of contingency, disaster recovery and restore management

Implemented control environment
The implemented controls are based on the services provided by COMBY A/S to customers and include control areas and control activities within operation and hosting. All of the above areas are described in detail in the following in separate paragraphs, and the described control objectives and controls for those areas in the paragraph on control objectives, controls, tests and result of tests are an integral part of the description.

A.5 Information security policy
COMBY A/S has drawn up a formal information security policy with accompanying instructions. It is provided in connection with employment and all employees are also required to ensure they are updated periodically in relation to information security policy and the related manuals. Policies are approved annually, and manuals are approved when material changes are made. Finally, our suppliers/business partners are made familiar with the information security policy when obtaining non-disclosure agreements. The information security policy is reassessed annually by the Management.

A.6 Organisation of information security
COMBY A/S has implemented controls to ensure a general management of the information security including a delegation of responsibilities and handling of material risks in accordance with the requirements of the company's Management.

Management's obligations in relation to information security
Management takes an active part in the IT security in the organisation. The formal responsibility, including approval of the information security policy, is that of the combined C-level and is led by the IT Security Responsible.

Placing of responsibility for information security
All areas of responsibility for the IT security are described in COMBY A/S' security policy which clearly describes where the responsibility is placed in relation to information security and the contingency planning.

Placing of responsibility for data protection
The business' CEO is always responsible for the data protection. Management has delegated this responsibility to the IT Security Responsible of the business. The IT Security Responsible manages together with staff the operational responsibility for complying with personal data protection, internally and in relation to customer data.

Mobile data processing and communication
COMBY A/S' staff manual sets out guidelines for use of mobile equipment outside the company. Only equipment, which complies with COMBY A/S' security policy, can access the network from the outside and exclusively via VPN.

All remote work can solely be performed via our authorised PCs. Access from home workplace is secured via encrypted VPN connection, which requires validation via Active Directory.

Authentication of users on external connections
All access to our network, including external users, is authorised by our formal Access Management procedure.

Non-approved user equipment
Guest equipment and non-approved equipment, for example mobile phones, can solely be connected to a separate guest network.

A.7 Human resource security
COMBY A/S has implemented controls to ensure that employees are qualified and conscious of their tasks and responsibilities in relation to information security.

For the purpose of employment at COMBY A/S, operational staff with access to customer data are subject to internal security clearance granted at the time of hiring.

Management's responsibility
As regards employees, they commit themselves, at their employment, to comply with the company's policies, including the security policy.

Awareness of information security and data protection, education and training
As regards employees, they are informed of all material changes to applicable policies and relevant procedures. This is done partly at the reoccurring IT awareness activities and through information about updates to policies and procedures that are delivered through different channels like e-mail, staff meetings, and automated messages about updates procedures and processes.

The employees are currently informed of personal data protection, so that there is a constant awareness of how employees manage the work with personally identifiable data, their own as well as the customers' data.

Roles and responsibilities
The responsibilities of the employees follow their place in the organisation. The responsibilities of all roles in relation to IT security are described in information security policy.

Non-disclosure agreements
Confidentiality is part of the employment contracts, and all employees must sign a non-disclosure agreement.

Obligations relating to departures
General employment conditions are described in the employee's employment contract. Moreover, there is a formal procedure for departure which must be followed by the immediate manager. The HR manager has the ultimate responsibility in this respect.

Return of equipment
All employees are to return all received material when the employment contract ends. This is done through the procedure for employee departure, which is followed by the immediate manager. The responsibility for return of equipment lies with the HR manager.

Closing of access rights
COMBY A/S' formal HR procedures ensure that all rights and physical access are withdrawn when an employment ends. This is done through a workflow placed with the immediate manager.

Sanctions relating to breach of the information security
The information security policy describes the process for sanctions relating to breach of the information security. The workplace is subject to COMBY A/S' security routines which must not be broken.

A.8 Asset management
COMBY A/S has implemented controls to ensure achievement and maintenance of suitable protection of the organisation's equipment.

Registration of equipment
Relevant equipment, which is utilised, is registered in COMBY A/S' configuration management database (CMDB). Moreover, there is an updated list of all authorised equipment and the equipment's primary user.

Accepted use of equipment
The employees' use of IT equipment and data is subject to fixed guidelines, defined in COMBY A/S' information security manual.

Management of portable media
The rules for use of portable media are defined in COMBY A/S' staff manual.

A.9 Access management
COMBY A/S has implemented controls to ensure that access to systems and data are granted through a process in accordance with a relevant work-related need and is closed down when the relevant access is no longer necessary.

Guidelines for use of network services
All user rights, including access to network, drives and applications, are determined on the basis of their function.

Business-critical applications
Access to all internal business critical applications is protected with MFA in all cases where it is supported by the application. Privileged access to business-critical applications is reviewed yearly by the person responsible for the specific applications. Regular access to business-critical applications is reviewed twice a year by the person responsible for the specific applications

Extended rights
All rights are managed on the basis of the employees' roles and are reviewed yearly as described in COMBY A/S' information security policy.

Management of password
Granting of passwords is subject to a number of rules which are set out in our Active Directory. Passwords that grant access to customer data is subject to the rules which are defined by the customer, and in most cases are set in that customers Active Directory.

Reassessment of user access rights
All accesses and rights are reviewed periodically as described in the information security policy. The process and interval between the reviews differs for internal user rights, customer user rights and customer user rights for customers with heightened security.

User identification and authentication
COMBY A/S has separate admin-profiles for all operational staff on the internal systems where this is technically possible and for customers with heightened security. For customers without heightened security COMBY A/S do not use separate admin-profiles for the operational staff.

A.11 Physical and environment security
COMBY A/S has implemented controls to ensure that IT equipment is properly protected against unauthorised physical access and environmental incidents.

Physical access control
COMBY A/S' premises have access control in the form of a required personal key to ensure that only authorised staff have access. Only COMBY A/S employees and authorised external contractors receive a key.

Safeguarding of offices, premises, and facilities
COMBY A/S' premises have access control in the form of a required electronic key to ensure that only authorised staff and authorised external contractors have access. If suppliers, consultants, or other external parties without authorisation are to have access, this is only possible together with authorised personnel.

Public areas, loading and unloading areas
Public access is only possible in the reception area. All other access is possible only together with authorised staff.

Storing of equipment and protection of equipment
The critical equipment is placed in the server room to which only technical staff and COMBY A/S partners have access.

A.12 Operations security
COMBY A/S has implemented controls to ensure that operation of servers and key systems is carried out in a structured and secure manner.

Documented operating procedures
All operating procedures are included in COMBY A/S' documentation management system and are therefore easily available to all staff through the portal.

Safeguarding of systems documentation
COMBY A/S keeps the systems documentation centrally in our documentation management system, which can solely be accessed by authorised staff.

Control of procedures for changes
We have a formal internal procedure for change management, which is based in our service desk system. By default, customers do not have a formal procedure for change management unless explicitly required by each specific customer.

Management of capacity
Monitoring of capacity has been implemented in relation to network, servers, and disk space. COMBY A/S reports on capacity on all customers where this is a part of delivered services and are used in the planning of purchase of additional capacity.

Backup of information
Backup is taken of all important data according to customer agreements made. Errors in backup are identified by the Event team and registered in COMBY A/S' service desk. Restore test for the customer is performed only when a specific agreement exists between the customer and COMBY A/S.

Control of malicious code
All registered servers in COMBY A/S' infrastructure is updated with approved antivirus software. All workstations in COMBY A/S are updated with approved antivirus software. New workstations are installed with a standard image, which automatically installs the required antivirus software.

Audit log
For customers with heightened security the access to syslog is limited so that regular privileged accounts do not have access to tamper with syslog. For other customers user transactions, exceptions and security incidents are logged with the default windows/Linux logging, and the log is stored according to the default retention periods.

Use of monitoring systems
COMBY A/S has implemented an internal event monitoring system to ensure that events are addressed in order to respond to relevant incidents and act accordingly. All events are reviewed by the event team and if needed, cases are created on the basis hereof.

Incident logging
All incidents are registered in COMBY A/S' IT Service Management System. Incidents concerning breach in relation to the processing of personal data are always marked, so that they can rapidly be identified and dealt with by COMBY A/S' IT Security Responsible.

A.13 Communications security
COMBY A/S has implemented controls to ensure that operation of material infrastructure components is carried out in a structured and secure manner.

Network controls
COMBY A/S has written guidelines for configuration of firewalls, routers, and switches, which are solely carried out by the operations department.

Security services on the network
Access to COMBY A/S' systems for our customers goes either through public networks where access is via VPN and firewall. Access and communication between our servers and the internet go through our centrally managed firewall. All incoming network traffic goes through our firewalls. Only approved network traffic is allowed through the firewall based on a customer request.

Control of network connections
Customer networks are limited by the VLAN and Access rules in our Core router / firewall.

A.16 Information security incident management
COMBY A/S has established controls and guidelines which ensure that incidents are dealt with in time and that there is a follow-up on the incidents.

All incidents, including security incidents, follow our formal Incident/Problem Management or Request Fulfilment procedure. These are based on our service desk system.

COMBY A/S has implemented procedures for documentation of all breaches of the management of personal data, which includes identification of the" root cause" of the breach, contact with authorities and corrective measures. All procedures are available to employees with a functional need.

A.17 Information security aspects of contingency, disaster recovery and restore management
COMBY A/S has prepared a contingency plan which is updated as required.

Information security integrated in the contingency plan
COMBY A/S has a formal contingency plan in which information security is incorporated.

Development and implementation of contingency plans which include information security
We have developed contingency plans to maintain or restore operations and ensure access to data at the required level and within acceptable time after failure or outage of critical business processes.

Responsibilities and guidelines
Roles and responsibilities are defined in the contingency plan.

Contingency plan
COMBY A/S assesses risks, and the contingency plan is updated to the existing risk exposure at least once a year or in connection with large changes to the entire solution and/or security policy.

Testing, maintenance, and reassessment of contingency plans
The contingency plan is tested as described in the contingency plans to ensure that it is applicable, sufficient, and effective.

4. CONTROL OBJECTIVES, CONTROLS, TEST AND RESULTS OF TESTS

Objective and scope

BDO has carried out the work in accordance with ISAE 3402 on assurance engagements relating to controls at a service organisation.

BDO has performed procedures to obtain evidence of the information in COMBY A/S' description of hosted and managed services and the design and implementation of these controls. The procedures performed depend on BDO's assessment, including the assessment of the risks that the description is not fairly presented and that the controls are not suitably designed.

BDO's test of the design of controls has included the control objectives and related control activities selected by COMBY A/S, and which are described in the following.

In the check form, BDO has described the tests performed which were considered necessary to obtain a reasonable degree of assurance that the stated control objectives were achieved and that the related controls were suitably designed on November 30 2022.

Test procedures

Tests of the design of technical and organisational security measures and other controls, the implementation and effectiveness hereof were performed by inquiry, inspection, observation and re-performance.

Type	Description
Inquiry	Inquiries of relevant personnel at COMBY A/S have been performed for all significant control activities. The purpose of the inquiries was to obtain knowledge and further information about implemented policies and procedures, including how the control activities are performed, and to obtain confirmed evidence of policies, procedures, and controls.
Inspection	Documents and reports, which include information about the performance of the control, have been read for the purpose of assessing the design and monitoring of the specific controls, i.e. whether the design of the controls is such that they are expected to be effective if implemented, and whether the controls are sufficiently monitored and checked at suitable intervals. Tests have been performed of significant system structures of technical platforms, databases, and network equipment to ensure that controls have been implemented, including for example assessment of logging, back-up, patch management, authorisations and access controls, data transmission, and inspection of equipment and locations.
Observation	The use and existence of specific controls have been observed, including tests to ensure that the control has been implemented.

For the services provided by Interxion Danmark ApS within hosted and managed services, we have from an independent auditor received a SOC 2 report for the period from 1 January 2021 to 31 December 2021 on technical and organisational security measures relating to operation of Cloud Backup services.

This sub-service provider's relevant control objectives and related controls are not included in COMBY A/S' description of services and relevant controls related to operation of COMBY A/S' Outsourcing Services. Accordingly, we have solely assessed the report and tested the controls at COMBY A/S that monitor the operating effectiveness of the sub-service provider's controls.

Result of test

The result of the test made of technical and organisational measures and other controls has resulted in the conclusions specified on the following pages.

An exception exists when:

- Technical and organisational measures and other controls have not been designed or implemented to fulfil a control objective,
- Technical and organisational measures and other controls related to a control objective are not suitably designed and implemented.

A.5: Information security policies

Control objectives

- *To provide guidelines for and support information security in accordance with business requirements and relevant laws and regulations.*

Control activity	Test performed by BDO	Result of test
Policies for information security ▶ A set of policies for information security should be defined, approved by management, published, and communicated to employees and relevant external parties.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's information security policy. We have observed that the information security policy is structured according to ISO 27001. We have inspected that the information security policy is approved by the management. We have observed that the information security policy is communicated to employees and relevant external cooperative partners.	No exceptions noted.
Review of policies for information security ▶ The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's annual cycle and observed that the information security policy must be reviewed once a year. We have observed that it has been reviewed during 2022.	No exceptions noted.

A.6: Organisation of information security and internal organisation

Control objectives

- *To establish a managerial basis to initiate and control the implementation and operation of information security in the organisation.*
- To ensure that employees and contractors understand their responsibilities and are suited to the roles for which they are intended.

Control activity	Test performed by BDO	Result of test
Information security roles and responsibilities ▶ All information security responsibilities should be defined and allocated.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for organisation of information security and observed that the service provider has defined and divided all areas of responsibility for information security.	No exceptions noted.
Segregation of duties ▶ Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for segregation of duties and observed that the service provider by random samples controls to ensure segregation of duties.	No exceptions noted.
Contact with authorities ▶ The appropriate contacts with relevant authorities should be maintained.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for contact with authorities and observed that a list of relevant authorities has been defined. By request we have been informed that the service provider has not been in contact with any relevant authorities.	No exceptions noted.
Mobile device policy ▶ A policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices.	We have made inquiries with relevant personnel at the service provider.	No exceptions noted.

A.6: Organisation of information security and internal organisation		
Control objectives ▶ *To establish a managerial basis to initiate and control the implementation and operation of information security in the organisation.* ▶ To ensure that employees and contractors understand their responsibilities and are suited to the roles for which they are intended.		
Control activity	**Test performed by BDO**	**Result of test**
	We have inspected the service provider's procedure for mobile devices. We have observed that laptops are locked with password and that a permanent lock is activated by multiple failed login attempts. By random sampling, we have inspected the service provider's employee's laptops and observed that automatic updating is configured in accordance with the Processor's procedure for this. We have inspected the service provider's set-up of remote access and observed that the remote access go through an encrypted VPN connection with 2 factor authentication.	
Teleworking ▶ A policy and supporting security measures should be implemented to protect information accessed, processed or stored at teleworking sites.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for teleworking. By request we have been informed that remote access is not allowed with unapproved tools.	No exceptions noted.

A.7: Employee safety

Control objectives

- *To ensure that employees and contractors understand their responsibilities and are suited for the roles for which they are intended.*
- *Ensuring employees and contractors are aware of and live up to their information security responsibilities.*
- *To protect the interests of the organisation as part of the change or termination of the employment relationship*

Control activity	Test performed by BDO	Result of test
Screening ▶ Background verification checks on all candidates for employment should be carried out in accordance with relevant laws, regulations and ethics and should be proportional to the business requirements, the classification for the information to be accessed and the perceived risks.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for employing new employees and observed that the service provider has established a process for screening new employees. By random sampling we have inspected documentation that a new employee has been through the screening process and observed that the process has been completed.	No exceptions noted.
Terms and conditions of employment ▶ The contractual agreements with employees and contractors should state their and the organisation's responsibilities for information security.	We have made inquiries with relevant personnel at the service provided and observed that the employees' responsibilities are defined. We have inspected the service provider's procedure for terms and conditions of employment By request we have been informed that all employees have signed a confidentiality agreement. By random sampling we have inspected that an employee has signed the confidentiality agreement and the information security policy.	No exceptions noted.
Management responsibilities ▶ Management should require all employees and contractors to apply information security in accordance with the established policies and procedures of the organisation.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for management responsibilities and observed that all employees must be presented with established policies and procedures	No exceptions noted.

A.7: Employee safety

Control objectives

- *To ensure that employees and contractors understand their responsibilities and are suited for the roles for which they are intended.*
- *Ensuring employees and contractors are aware of and live up to their information security responsibilities.*
- *To protect the interests of the organisation as part of the change or termination of the employment relationship*

Control activity	Test performed by BDO	Result of test
	By random sampling we have inspected that employees are signing a declaration regarding compliance with the employee handbook and the information security policy. We have observed that the management participates in the information security awareness activities.	
Information security awareness, education, and training ▶ All employees of the organisation and, where relevant, contractors should receive appropriate awareness education and training as well as regular updates in organisational policies and procedures, as relevant for their job function.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for awareness, education and training and observed that semi-annual activities are made. We have inspected that all employees have completed the general awareness activities. By random sampling we have inspected that employees have completed appropriate awareness activities.	No exceptions noted.
Disciplinary process ▶ There should be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for disciplinary process and observed that employees may be sanctioned by breaching the information security. We have inspected that employees are informed about the disciplinary procedure in the employee handbook. By request we have been informed that there have not been any information security breaches. Thus, we have not been able to test the control.	No exceptions noted.

A.7: Employee safety

Control objectives

- *To ensure that employees and contractors understand their responsibilities and are suited for the roles for which they are intended.*
- *Ensuring employees and contractors are aware of and live up to their information security responsibilities.*
- *To protect the interests of the organisation as part of the change or termination of the employment relationship*

Control activity	Test performed by BDO	Result of test
Termination or change of employment responsibilities ▶ Information security responsibilities and duties that remain valid after termination or change of employment should be defined, communicated to the employee or contractor and enforced.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for termination or change of employment responsibilities and observed that defines who and what are to happen when an employee is to stop. We have inspected that the service provider has a template for termination of employees who have been notified that the confidentiality agreement applies after resignation. By inquiry, we have been informed that the service provider is working on a similar template for when an employee resigns. By random sampling we have inspected that a resignation has followed the procedure, including that the employee has returned received assets and access rights have been closed.	No exceptions noted.

A.8: Asset Management

Control objectives

- *To identify the organisation's assets and define appropriate responsibilities for its protection.*
- *To ensure appropriate protection of information that is in proportion to the importance of the information to the organisation.*
- *To prevent unauthorised publication, alteration, removal, or destruction of information stored on media.*

Control activity	Test performed by BDO	Result of test
Inventory of assets ▶ Assets associated with information and information processing facilities should be identified and an inventory of these assets should be drawn up and maintained.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for inventory management and observed that an inventory of assets must be in place. We have inspected the inventory of assets and observed that it is continuously reviewed. By random sampling we have controlled that distributed assets are in accordance with the inventory of assets.	No exceptions noted.
Ownership of assets ▶ Assets maintained in the inventory should be owned.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for owner ship of assets and observed that each asset must assigned to an owner. We have inspected the inventory of assets and observed that each asset is assigned an owner.	No exceptions noted.
Accepted use of assets ▶ Rules for the acceptable use of information and of assets associated with information and information processing facilities should be identified, documented and implemented.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's employee handbook and observed that acceptable and unacceptable use of assets have been defined.	No exceptions noted.

A.8: Asset Management

Control objectives

- *To identify the organisation's assets and define appropriate responsibilities for its protection.*
- *To ensure appropriate protection of information that is in proportion to the importance of the information to the organisation.*
- *To prevent unauthorised publication, alteration, removal, or destruction of information stored on media.*

Control activity	Test performed by BDO	Result of test
	By request we have been informed that all employees have been introduced to the employee handbook.	
Return of assets ▶ All employees and external party users should return all of the organisational assets in their possession upon termination of their employment, contract or agreement.	We have made inquiries with relevant personnel at the service provider. We have inspected that the service provider's procedure for return of assets and observed that assets must be returned when an employee resigns. By random sampling we have inspected that a resigned employee has returned all assets in accordance with the procedure. By request we have been informed that the service provider has not distributed assets to external parties. Thus, we have not been able to test the control.	No exceptions noted.
Disposal of media ▶ Media should be disposed of securely when no longer required, using formal procedures.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for disposal of medias and observed that medias are disposed different depending on the type of media. By request we been informed that the service provider has not disposed any media yet. Thus, we have not been able to test the control.	No exceptions noted.

A.9: Access Management

Control objectives

- *To restrict access to information and information processing facilities.*
- *To ensure access for authorised users and prevent unauthorised access to systems and services.*
- *To prevent unauthorised access to systems and applications.*

Control activity	Test performed by BDO	Result of test
Access control policy ▶ An access control policy should be established, documented and reviewed based on business and information security requirements.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for access control and observed that it is reviewed annually. We have observed that it has been reviewed during 2022.	No exceptions noted.
Access to networks and network services ▶ Users should only be provided with access to the network and network services that they have been specifically authorised to use.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for access control and observed that access is provided in three different groups. By random sampling we have inspected that an employee is only provided with access when a specific authorisation is in place. We have inspected that the service provider performs quarterly controls of which users have established access through VPN.	No exceptions noted.
User registration and deregistration ▶ A formal user registration and de-registration process should be implemented to enable assignment of access rights.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for access control and observed that each employee is provided their own individual user. We have tested that a user is forced to change password at first login.	No exceptions noted.

A.9: Access Management

Control objectives

- *To restrict access to information and information processing facilities.*
- *To ensure access for authorised users and prevent unauthorised access to systems and services.*
- *To prevent unauthorised access to systems and applications.*

Control activity	Test performed by BDO	Result of test
	We have inspected that the service provider performs controls to ensure the deletion of inactive users and that no common users have been created.	
User access provisioning ▶ A formal user access provisioning process should be implemented to assign or revoke access rights for all user types to all systems and services.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for access control and observed that user access is defined on three different levels, hereunder internal, customer and customer with heightened security. By random sampling we have inspected that assigning of users regarding customers with heightened security has been in accordance with the procedure.	No exceptions noted.
Management of privileged access rights ▶ The allocation and use of privileged access rights should be restricted and controlled.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for access control and observed that user management of privileged access rights is defined on three different levels, including internal, customer and customer with heightened security. We have inspected that the service provider only has a limited number of users with privileged access rights. We have inspected that privileged access rights to customers with heightened security requires approval from the customer.	No exceptions noted.

A.9: Access Management

Control objectives

- *To restrict access to information and information processing facilities.*
- *To ensure access for authorised users and prevent unauthorised access to systems and services.*
- *To prevent unauthorised access to systems and applications.*

Control activity	Test performed by BDO	Result of test
Management of secret authentication information of users ▶ The allocation of secret authentication information should be controlled through a formal management process.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for access control and observed that management of secret authentication information of users is defined on three different levels, hereunder internal, customer and customer with heightened security. We have inspected that users are forced to change password after their first login. We have further inspected that a new temporary password is forced to change after first login.	No exceptions noted.
Review of user access rights ▶ Asset owners should review users' access rights at regular intervals.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for access control and observed that review of user access rights is defined on three different levels, hereunder internal, customer and customer with heightened security. We have inspected that the service provider annually reviews the users access rights. We have inspected that the service provider reviews that domain admins at customers with heightened security has been assigned in accordance with the procedure.	No exceptions noted.
Removal or adjustment of access rights ▶ The access rights of all employees and external party users to information and information processing facili-	We have made inquiries with relevant personnel at the service provider.	No exceptions noted.

A.9: Access Management

Control objectives

- *To restrict access to information and information processing facilities.*
- *To ensure access for authorised users and prevent unauthorised access to systems and services.*
- *To prevent unauthorised access to systems and applications.*

Control activity	Test performed by BDO	Result of test
ties should be removed upon termination of their employment, contract or agreement, or adjusted upon change.	We have inspected the service provider's procedure for access control and observed that removal or adjustment of access rights is defined on three different levels, hereunder internal, customer and customer with heightened security. By random sampling we have inspected that a resignation has followed the procedure, hereunder that the former employee's access rights have been closed for all types of customers.	
Use of secret authentication information ▶ Users should be required to follow the organisation's practices in the use of secret authentication information.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for access control and observed that all users must comply with the service provider's password policy. We have observed that the passwords policy is implemented. We have further inspected that forced two-factor authentication is implemented. We have inspected that the service provider performs an annual control to ensure that the password policy is adequate in accordance with the identified risks.	No exceptions noted.
Information access restriction ▶ Access to information and application system functions should be restricted in accordance with the access control policy.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for access control and observed that user access rights have been defined and implemented.	No exceptions noted.

A.9: Access Management

Control objectives

- *To restrict access to information and information processing facilities.*
- *To ensure access for authorised users and prevent unauthorised access to systems and services.*
- *To prevent unauthorised access to systems and applications.*

Control activity	Test performed by BDO	Result of test
Secure log-on procedures ▶ Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for access control and observed that secure log-on is defined. We have tested that two-factor authentication is implemented. We have observed that laptops are locked with password and that a permanent lock is activated multiple failed login attempts. We have inspected that the service provider annually controls that the two-factor authentication is active and effective. We have inspected that the service provider reviews the log of failed login attempts.	No exceptions noted.
Password management system ▶ Password management systems should be interactive and should ensure quality passwords.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for access control and observed that the service provider controls which password a user has applied. We have reviewed the log of logins and have been informed that users only have had access to passwords they specifically have been authorised to use.	No exceptions noted.

A.9: Access Management

Control objectives

- *To restrict access to information and information processing facilities.*
- *To ensure access for authorised users and prevent unauthorised access to systems and services.*
- *To prevent unauthorised access to systems and applications.*

Control activity	Test performed by BDO	Result of test
Use of privileged system programs ▶ The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly and controlled.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for access control and observed that the system owner is responsible for ensuring that unwanted utility programs are not installed. We have inspected that the service provider controls that utility programs might be capable of overriding systems.	No exceptions noted.

A.11: Physical protection and environmental protection

Control objectives

- *To ensure that procedures exist for accessing* the service provider's *sites and that sites are classified.*
- *To ensure a stable supply to* the service provider*'s locations.*
- *To ensure that there is no unauthorised access to* the service provider's *sites.*

Control activity	Test performed by BDO	Result of test
Physical security perimeter ▶ Security perimeters should be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for physical security and observed that it defines the physical security perimeter. By request, we have been informed that intruder alarms are active on all locations, and that no break-ins have taken place. We have inspected that entry control is active and that entries are logged. By random sampling, we have inspected logs of physical entries. We have inspected that the service provider obtains Interxion's SOC 2 report to ensure the security of their external data centre. We have inspected that the service provider annual tests their alarms and physical entry controls, and we have observed that the tests were completed.	We have noted that the alarm system in Greenland does not work effectively. We have been informed that this is being rectified. No further exceptions noted.
Physical entry control ▶ Secure areas should be protected by appropriate entry controls to ensure that only authorised personnel are allowed access. All accesses are registered and logged.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for physical security and observed that secure areas which requires physical entry control have been defined. We have inspected that only a limited number of employees have access to their data centres.	No exceptions noted.

A.11: Physical protection and environmental protection		
Control objectives ▶ *To ensure that procedures exist for accessing* the service provider's *sites and that sites are classified.* ▶ *To ensure a stable supply to* the service provider*'s locations.* ▶ *To ensure that there is no unauthorised access to* the service provider's *sites.*		
Control activity	**Test performed by BDO**	**Result of test**
	We have inspected that active video surveillance is installed at the data centre in Greenland.	
Securing offices, rooms, and facilities ▶ Physical security for offices, rooms and facilities should be designed and applied.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for physical security and observed that a clean desk policy is defined. We have inspected that the service provider controls that confidential information and documents are not left unattended. We have inspected that the service provider controls that automatic screen lock is active and configurated.	No exceptions noted.
Protection against external and environmental threats ▶ Physical protection against natural disasters, malicious attack or accidents should be designed and applied.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for physical security and observed that it defines the protections against external and environmental threats. By request, we have been informed that the service provider has a redundant setup to ensure that the employees can access relevant systems in case of a breach at one location. We have inspected that the service provider controls that the overall physical security is adequate.	No exceptions noted.
Working in secure areas ▶ Procedures for working in secure areas should be designed and applied.	We have made inquiries with relevant personnel at the service provider.	No exceptions noted.

A.11: Physical protection and environmental protection

Control objectives

- *To ensure that procedures exist for accessing* the service provider's *sites and that sites are classified.*
- *To ensure a stable supply to* the service provider*'s locations.*
- *To ensure that there is no unauthorised access to* the service provider's *sites.*

Control activity	Test performed by BDO	Result of test
	We have inspected the service provider's procedure for physical security and observed that it defines the service provider's secure working areas. We have inspected the list of safety approved employees and by request we have been informed that it is correct. We have inspected that the service provider performs an annual control to ensure that the safety approved employees are correct.	
Equipment siting and protection - Equipment should be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for physical security and observed that it defines equipment siting and protection. We have inspected that working stations are protected from unauthorised access.	No exceptions noted.
Supporting utilities - Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for physical security and observed that an UPS shall be setup. We have inspected that an UPS is setup on all location and that the service provider services the UPS in accordance with their procedure.	No exceptions noted.

A.11: Physical protection and environmental protection

Control objectives

- *To ensure that procedures exist for accessing* the service provider's *sites and that sites are classified.*
- *To ensure a stable supply to* the service provider*'s locations.*
- *To ensure that there is no unauthorised access to* the service provider's *sites.*

Control activity	Test performed by BDO	Result of test
Cabling security ▶ Power and telecommunications cabling carrying data or supporting information services should be protected from interception, interference, or damage.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for physical security and observed that all power and telecommunications cabling is routed underground and shielded in safe boxes at entrances. By request, we have been informed that all power and telecommunications cabling is routed underground and at building entrances they are shielded in safe boxes.	No exceptions noted.
Equipment maintenance ▶ Equipment should be correctly maintained to ensure its continued availability and integrity.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for physical security and observed that the service provider services the fire extinguishing system, UPS, and servers. We have inspected that the fire extinguishing system, UPS, and servers must be serviced by the service provider.	We have noted that the service provider has not yet serviced the fire extinguishing system. No further exceptions noted.
Security of equipment and assets off-premises ▶ Security should be applied to off-site assets taking into account the different risks of working outside the organisation's premises.	We have made inquiries with relevant personnel at the service provider. We have inspected that all laptops have two-factor authentication configurated. By request, we have been informed that it is not allowed to bring physical documents outside of office areas.	No exceptions noted.

A.11: Physical protection and environmental protection

Control objectives

- *To ensure that procedures exist for accessing* the service provider's *sites and that sites are classified.*
- *To ensure a stable supply to* the service provider*'s locations.*
- *To ensure that there is no unauthorised access to* the service provider's *sites.*

Control activity	Test performed by BDO	Result of test
Clear desk and clear screen policy ▶ A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for physical security and observed that a clear desk policy has been defined. By request, we have been informed that physical documents containing confidential information must not be left unattended and must be kept in locked cabinets. We have inspected that automatic screen lock is active and configurated.	No exceptions noted.

A.12: Operations Security

Control objectives

- *To ensure proper and safe operation of information processing facilities.*

Control activity	Test performed by BDO	Result of test
Documented and operating procedures ▶ Operating procedures should be documented and made available to all users who need them.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for operations security. We have inspected that the service provider has a log of operational irregularities. By random sampling we have inspected that the service provider has implemented standard operations procedures and customer specific operations procedures.	No exceptions noted.
Change management ▶ Changes to the organisation, business processes, information processing facilities and systems that affect information security should be controlled.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for operations security and observed that it defines change management. By request, we have been informed that changes must go through a formalised approval procedure before operation. We have inspected their flow chart for change management and observed that a change starts with a change request. By random sampling, we have inspected that a change request has been completed in accordance with the procedure. We have inspected that the service provider reviews the change management procedure. By request we have been informed that the service provider has no customer specific change management procedures.	No exceptions noted.

A.12: Operations Security

Control objectives

- *To ensure proper and safe operation of information processing facilities.*

Control activity	Test performed by BDO	Result of test
Capacity management ▶ The use of resources should be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for operations security and observes that it defines capacity management. We have inspected that the service provider is monitoring so that upgrade can take place continuously. By random sampling, we have inspected that an alarm is received and handled in accordance with the procedure.	No exceptions noted.
Controls against malware ▶ Detection, prevention, and recovery controls to protect against malware should be implemented, combined with appropriate user awareness.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for operations security and observes that it defines controls against malware. By random sampling, we have inspected that laptops have antivirus installed and that it is automatically updated. By random sampling, we have inspected antivirus report for customers.	No exceptions noted.
Information backup ▶ Backup copies of information, software and system images should be taken and tested regularly in accordance with an agreed backup policy.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for operations security and observed that it defines information backup, and that backup is daily.	No exceptions noted.

A.12: Operations Security		
Control objectives ▶ *To ensure proper and safe operation of information processing facilities.*		
Control activity	**Test performed by BDO**	**Result of test**
	By random sampling, we have inspected that the service provider handles a failed backup. By random sampling, we have inspected that restore tests on customer's data are performed. We have inspected a backup report for customers.	
Administrator and operator log ▶ System administrator and system operator activities should be logged, and the logs are protected and regularly reviewed.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for operations security and observed that it defines logging. By request, we have been informed that logging is only relevant for specific customers. By random sampling, we have inspected that the log is active for customers.	No exceptions noted.
Management of technical vulnerabilities ▶ Information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organisation's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for operations security and observed that it defines management of technical vulnerabilities. We have inspected that the service provider conducts a prioritised list of vulnerabilities in their own systems. We have inspected that the service provider conducts vulnerability reports to customers containing a prioritised list of vulnerabilities.	No exceptions noted.

A.12: Operations Security		
Control objectives ▶ *To ensure proper and safe operation of information processing facilities.*		
Control activity	**Test performed by BDO**	**Result of test**
	By random sampling, we have inspected that identified vulnerabilities have been handled.	

A.13: Communication security

Control objectives

- *To ensure the protection of information in networks and of supporting information processing facilities.*

Control activity	Test performed by BDO	Result of test
Network controls ▶ Networks should be managed and controlled to protect information in systems and applications.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for communication security and observed that network controls are defined. By request we have been informed that all external communication links shall be approved. We have inspected that the networks are protected by firewalls. We have inspected the service provider's network diagrams. We have inspected that only a limited number of employees have access to switchboards.	No exceptions noted.
Security of network services ▶ Security mechanisms, service levels and management requirements of all network services should be identified and included in network services agreements, whether these services are provided inhouse or outsourced.	We have made inquiries with relevant personnel at the service provider. We have inspected the service provider's procedure for communication security and observed that security of network services is defined. We have inspected the service provider's negative list of web-based services. We have inspected the service provider's list of approved remote access tools.	No exceptions noted.

A.16: Management of information security breaches

Control objectives

- *To ensure a uniform and effective method of managing information security breaches, including communication of security incidents and vulnerabilities.*

Control activity	Test performed by BDO	Result of test
Responsibilities and procedures ▶ Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to information security incidents.	We have interviewed relevant personnel with the service provider. We have inspected the service provider's procedure for management of information security breaches and observed that the responsibilities have been defined. We have inspected that the service provider annually reviews the procedure for management of information security breaches.	No exceptions noted.
Reporting information security incidents ▶ Information security events should be reported through appropriate management channels as quickly as possible.	We have interviewed relevant personnel with the service provider. We have inspected the service provider's procedure for management of information security breaches and observed that the service provider has defined how the reporting shall be. We have inspected that all employees have completed awareness activities regarding incident management. We have inspected the service provider's incident log and observed that no incidents have been registered. Thus, we have not tested the control.	No exceptions noted.
Assessment of and decision on information security events ▶ Information security events should be assessed, and it should be decided if they are to be classified as information security incidents	We have interviewed relevant personnel with the service provider.	No exceptions noted.

A.16: Management of information security breaches		
Control objectives ▶ *To ensure a uniform and effective method of managing information security breaches, including communication of security incidents and vulnerabilities.*		
Control activity	**Test performed by BDO**	**Result of test**
	We have inspected the service provider's procedure for management of information security breaches and observed that assessment of and decision on information security events is defined. We have inspected the service provider's incident log and observed that no incidents have been registered. Thus, we have not been able to tests the control.	
Response to information security incidents ▶ Information security incidents should be responded to in accordance with the documented procedures.	We have interviewed relevant personnel with the service provider. We have inspected the service provider's procedure or management of information security breaches and observed that response to information security incidents is defined. We have inspected the service provider's incident log and observed that no incidents have been registered. Thus, we have not been able to test the control.	No exceptions noted.

A.17: Information security aspects of emergency, emergency and re-establishment management		
Control objectives ▶ *To ensure a uniform and effective method of managing information security breaches, including communication of security incidents and vulnerabilities.*		
Control activity	**Test performed by BDO**	**Result of test**
Planning information security continuity ▶ The organisation should determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.	We have interviewed relevant personnel with the service provider. We have inspected the service provider's procedure for information security aspects of emergency. We have inspected that the service provider has a contingency plan. We have inspected that the service provider has a procedure in case of a major incident procedure. By request, we have been informed that there have not been any major incidents. Thus, we have not tested the control.	No exceptions noted.
Implementing information security continuity ▶ The organisation should establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	We have interviewed relevant personnel with the service provider. We have inspected the service provider's procedure for information security aspects of emergency. By request, we have been informed that the service provider does not have customers with a specific contingency plan. Thus, we have not been able to test the control. We have inspected that the service provider annually reviews business contingency plan to ensure its efficiency.	No exceptions noted.
Verify, review, and evaluate information security continuity ▶ The organisation should verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.	We have interviewed relevant personnel with the service provider. We have inspected the service provider's procedure for information security aspects of emergency.	No exceptions noted.

A.17: Information security aspects of emergency, emergency and re-establishment management		
Control objectives ▶ *To ensure a uniform and effective method of managing information security breaches, including communication of security incidents and vulnerabilities.*		
Control activity	**Test performed by BDO**	**Result of test**
	We have inspected that the service provider tests the contingency plan, and that adjustments were made as following evaluation.	

5. SUPPLEMENTARY INFORMATION FROM COMBY A/S

The supplementary information below has not been the subject of the audit carried out by BDO.

Based on BDO's ascertained exceptions in the ISAE 3402 declaration, COMBY A/S has the following supplementary information:

Control activity	Result of test	Comment of the company
Physical security perimeter ▶ Security perimeters should be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	We have noted that the alarm system in Greenland does not work effectively. We have been informed that this is being rectified.	Following the auditor testing of the control activity, corrective measures were taken to address the exception with the alarm system in Greenland. These efforts have resulted in the successful functioning of the alarm system.
Equipment maintenance ▶ Equipment should be correctly maintained to ensure its continued availability and integrity.	We have noted that the service provider has not yet serviced the fire extinguishing system.	COMBY A/S has yet to find a suitable subcontractor to maintain the fire extinguishing system. As a result, the company is currently in negotiations with potential subcontractors to replace and service the system in the future.

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

KYSTVEJEN 29
8000 AARHUS C

CVR-NR. 20 22 26 70

PENNEO

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registereret, og informationerne er listet herunder.

"Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument."

Stefan Grøndahl Boel
Chief Operating Officer
På vegne af: COMBY A/S
Serienummer: PID:9208-2002-2-581664468281
IP: 80.208.xxx.xxx
2023-01-24 12:02:20 UTC
NEM ID

Mikkel Jon Larssen
Partner, Head of Risk Assurance, CISA, CRISC
På vegne af: BDO Statsautoriseret revisionsaktiesels…
Serienummer: CVR:20222670-RID:52744874
IP: 77.243.xxx.xxx
2023-01-24 12:16:12 UTC
NEM ID

Nicolai Tobias Visti Pedersen
Partner, State Authorised Public Accountant
På vegne af: BDO Statsautoriseret Revisionsaktiesels…
Serienummer: CVR:20222670-RID:1283706411033
IP: 77.243.xxx.xxx
2023-01-24 14:53:59 UTC
NEM ID